


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

 Ad
Sc
Sc

Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 25 for [database intrusion detection IP](#)
All Results
[S CHARI](#)
[B Yee](#)
[P CHENG](#)
[H Tipton](#)
[K Fu](#)
[BlueBoX: A Policy-Driven, Host-Based Intrusion Detection System](#) - [all 13 versions »](#)

SN CHARI, PAUC CHENG - ACM Transactions on Information and System Security, 2003 - portal.acm.org

 ... maintain and update attack-signature **database** or statistic ... system resources such as **IPC** objects, sockets ... The Linux **Intrusion Detection** system (LIDS) [Xie and ...

[Cited by 60](#) - [Related Articles](#) - [Web Search](#)
[\[DOC\] A specification-based approach for intrusion detection](#)

Y Cai - 1999 - seclab.cs.sunysb.edu

 ... Kosoresow97] have developed an **intrusion detection** technique inspired ... **Intrusion** is detected when we observe "foreign ... to build up a separate **database** of normal ...

[Cited by 1](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)
[Supporting reconfigurable security policies for mobile programs](#) - [all 35 versions »](#)

B Hashii, S Malabarba, R Pandey, M Bishop - Computer Networks, 2000 - Elsevier

 ... adapting to varying system state, **intrusion**, and other ... For instance, a distributed in- trusion **detection** system may ... com to access a public **database** server, DBS ...

[Cited by 13](#) - [Related Articles](#) - [Web Search](#)
[\[PDF\] Acronyms, Initialisms, and Abbreviations](#) - [all 2 versions »](#)

DM JOHNSON - 2002 - osti.gov

 ... ADAM-advanced **database** and modeling ... AIDS-1. adaptive **intrusion** data system 2. automated

 information distribution ... ALDS-automatic lighting **detection** system ...

[View as HTML](#) - [Web Search](#)
[\[PDF\] Using Secure Coprocessors](#) - [all 19 versions »](#)

B Yee - 1994 - www-cse.ucsd.edu

 ... of the access control **database**, no system ... Physical **intrusion** by mechanical means (eg, drilling ... by National Semiconductor has tamper **detection** machinery which ...

[Cited by 250](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)
[2001: A Privacy Odyssey Revisited](#) - [all 2 versions »](#)

S Hinde - Computers & Security, 2001 - Elsevier

 ... which has been gathered by **intrusion detection** systems, which ... Such a **database**, once

 established, could be ... and creating an early warning **detection** network for ...

[Web Search](#)
[Automatic communication and security reconfiguration for remote services](#)

MJ Wookey, T Watson, J Chouanard - 2003 - freepatentsonline.com

 ... system's Inter-Process Communication (**IPC**) implementation with the ... for services, such as **database** persistency, high ... a creation of **detection**/collection logic ...

[Cached](#) - [Web Search](#)

[book] [Ethereal Packet Sniffing - all 4 versions »](#)

AD Orebaugh - 2004 - books.google.com

... Guide to Firewalls, VPNs, Routers, and Network **Intrusion Detection** by Stephen ...
Greg's

early roots in software development was in **database** technologies, dabbling ...

[Cited by 13](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[book] [Anti-hacker Tool Kit](#)

KJ Jones, BC Johnson, M Shema - 2002 - books.google.com

... and deployed high-capacity Apache Web and Oracle **database** serv- ers ... computer
networks,

such as firewalls, **intrusion-detection** systems, vulnerability and port ...

[Cited by 4](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[book] [Securing the US Defense Information Infrastructure: A Proposed Approach - all 4 versions »](#)

RH Anderson - 1999 - books.google.com

... partial matching algorithms (flexible **detection**); memory and ... DB **Database** DBMS
Database

management system ... IP Internet protocol **IPC** Interprocess communication ...

[Cited by 25](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

Google 

Result Page: 1 2 3 [Next](#)

database intrusion detection IPC int

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

[Ad](#)
[Sc](#)
[Sc](#)
Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 21 for **local database intrusion detecti**
All Results
[B Hashii](#)
[B Yee](#)
[R Anderson](#)
[S Norberg](#)
[S Malabarba](#)
[\[DOC\] A specification-based approach for intrusion detection](#)

Y Cai - 1999 - seclab.cs.sunysb.edu

... process P j to enforce the **local** security behavior ... **Intrusion** is detected when we observe "foreign" system call ... is to build up a separate **database** of normal ...

[Cited by 1](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)
[Supporting reconfigurable security policies for mobile programs - all 35 versions »](#)

B Hashii, S Malabarba, R Pandey, M Bishop - Computer Networks, 2000 - Elsevier
... adapting to varying system state, **intrusion**, and other ... and to verify consistency among the different **local** policies ... com to access a public **database** server, DBS ...

[Cited by 13](#) - [Related Articles](#) - [Web Search](#)
[\[PDF\] Acronyms, Initialisms, and Abbreviations - all 2 versions »](#)

DM JOHNSON - 2002 - osti.gov

... ADAM—advanced **database** and modeling ... AIDS—1. adaptive **intrusion** data system 2. automated ...

ALOE—analysis of **local** oriented edges (software developed by SNL ...

[View as HTML](#) - [Web Search](#)
[\[PDF\] Using Secure Coprocessors - all 19 versions »](#)

B Yee - 1994 - www-cse.ucsd.edu

... the integrity of the access control **database**, no system ... out how to tap into a **local** network using ... Physical **intrusion** by mechanical means (eg, drilling) cannot ...

[Cited by 250](#) - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)
[Automatic communication and security reconfiguration for remote services](#)

MJ Wookey, T Watson, J Chouanard - 2003 - freepatentsonline.com

... [0137] The **detection**/collection logic ... extracted from the remote services system **database**

through service ... checks to determine whether a **local** configuration does ...

[Cached](#) - [Web Search](#)
[\[BOOK\] Securing Windows NT/2000 Servers for the Internet - all 3 versions »](#)

S Norberg - 2000 - books.google.com

... Canada) (707) 829-0515 (international or **local**) (707) 829 ... **Intrusion** An intrusion occurs when an unauthorized person ... 3. The **database** software was running as root ...

[Cited by 9](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)
[\[BOOK\] Securing the US Defense Information Infrastructure: A Proposed Approach - all 4 versions »](#)

RH Anderson - 1999 - books.google.com

... partial matching algorithms (flexible **detection**); memory and learning ... Agency DB **Database**

DBMS **Database** management system ... service provider LAN **Local**-area network ...

[Cited by 25](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[\[book\] Ethereal Packet Sniffing - all 4 versions »](#)

AD Orebaugh - 2004 - books.google.com

... VPNs, Routers, and Network **Intrusion Detection** by Stephen ... Coach for the SANS **Local**Mentor Program ... in software development was in **database** technologies, dabbling ...[Cited by 13](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)[\[book\] Anti-hacker Tool Kit](#)

KJ Jones, BC Johnson, M Shema - 2002 - books.google.com

... and deployed high-capacity Apache Web and Oracle **database** serv- ers ... computer networks,such as firewalls, **intrusion-detection** systems, vulnerability and port ...[Cited by 4](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)[\[book\] Information Security Management Handbook - all 8 versions »](#)

HF Tipton, M Krause - 2003 - books.google.com

... 553 To Verify 555 Lab 81 : Capturing Switched Network Traffic 556

Intercept/Exploit Traffic: Ettercap Lab 82: Password Capture 573 ...[Cited by 53](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)Google Result Page: 1 2 3 [Next](#) [Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

intrusion detection IPC intercept

1994

- 2004

Search

Ad
Sc
Sc
Scholar All articles - **Recent articles** Results 1 - 10 of about 52 for **intrusion detection IPC intercept**
All Results[S CHARI](#)[B Yee](#)[P CHENG](#)[S Srinivasan](#)[H Tipton](#)
[BlueBoX: A Policy-Driven, Host-Based Intrusion Detection System - all 13 versions »](#)
[SN CHARI, PAUC CHENG - ACM Transactions on Information and System Security, 2003 - portal.acm.org](#)
[... other system resources such as IPC objects, sockets ... The Linux Intrusion Detection system \(LIDS\) \[Xie and Biondi ... systems with system call intercept-based systems ...](#)
[Cited by 60 - Related Articles - Web Search](#)
[\[DOC\] A specification-based approach for intrusion detection](#)
[Y Cai - 1999 - seclab.cs.sunysb.edu](#)
[... If all programs were designed with intrusion detection in mind, they ... behavioral specifications describing permissible event sequences, and intercept and verify ...](#)
[Cited by 1 - Related Articles - View as HTML - Web Search - Library Search](#)
[\[PDF\] Differential packet filtering against DDOS flood attacks - all 3 versions »](#)
[S Tanachaiwat, K Hwang - Proceedings of ACM Conference on Computer and Communications ..., 2003 - gridsec.usc.edu](#)
[... To stop future attacks, automated intrusion detection and response \(IDR ... problem, reconfigure the routers to intercept SYN attacks ... i , IPC i , T i \), where IP i ...](#)
[Cited by 7 - Related Articles - View as HTML - Web Search](#)
[\[PDF\] Network Working Group P. Srisuresh INTERNET-DRAFT Jasmine Networks Expires as of November 15, 2001 J ...](#)
[J Rosenberg, A Molitor, A Technologies, A Rayhan - Consultant, 2001 - tools.ietf.org](#)
[... NAT | DiffServ- | Intrusion | | | QOS | Detection | +--- Middlebox | Firewall ... transport such as IPC messaging \(or ...](#)
[View as HTML - Web Search](#)
[\[PDF\] Network Working Group P. Srisuresh INTERNET-DRAFT Jasmine Networks Expires as of December 13, 2001 J ... - all 2 versions »](#)
[J Rosenberg, A Molitor, A Technologies, A Rayhan - Consultant, 2001 - tools.ietf.org](#)
[... NAT | DiffServ- | Intrusion | | | QOS | Detection | +--- Middlebox | Firewall ... transport such as IPC messaging \(or ...](#)
[Related Articles - View as HTML - Web Search](#)
[\[PDF\] Network Working Group P. Srisuresh INTERNET-DRAFT Kuokoa Networks Expires as of June 17, 2002 J. ...](#)
[J Rosenberg, A Molitor, A Technologies, A Rayhan - Consultant, 2001 - tools.ietf.org](#)
[... NAT | VPN | Intrusion | | | tunneling | Detection | +--- Middlebox | Middlebox ... such as IPC messaging \(or ...](#)
[View as HTML - Web Search](#)
[\[PDF\] Network Working Group P. Srisuresh INTERNET-DRAFT Kuokoa Networks Expires as of August 28, 2002 J. ...](#)
[J Rosenberg, A Molitor, A Technologies, A Rayhan - Consultant, 2002 - tools.ietf.org](#)
[... NAT | VPN | Intrusion | | | tunneling | Detection | +--- Middlebox | Middlebox ... such as IPC messaging \(or ...](#)

[Related Articles](#) - [View as HTML](#) - [Web Search](#)

[PDF] [Network Working Group P. Srisuresh INTERNET-DRAFT Kuokoa Networks Expires as of April 4, 2002 J. ...](#) - [all 2 versions](#) »

J Rosenberg, A Molitor, A Technologies, A Rayhan - Consultant, 2001 - tools.ietf.org

... NAT | VPN | **Intrusion** | | | tunneling | **Detection** | +—

Middlebox | Firewall ACLs ... such as **IPC** messaging (or ...

[Related Articles](#) - [View as HTML](#) - [Web Search](#)

[Flashback: A Lightweight Extension for Rollback and Deterministic Replay for Software Debugging](#) - [all 8 versions](#) »

SM Srinivasan... - 2004 - unix.org

... In Flashback, we **intercept** system calls invoked by a ... shared memory for interprocess communication - System V **IPC** and BSD ... **Intrusion detection** via static analysis ...

[Cited by 48](#) - [Related Articles](#) - [Cached](#) - [Web Search](#) - [Library Search](#)

[Detecting exploit code execution in loadable kernel modules](#) - [all 9 versions](#) »

H Xu, W Du, SJ Chapin - Computer Security Applications Conference, 2004. 20th Annual, 2004 - ieeexplore.ieee.org

... For example, we **intercept** strcpy() to check whether ... to use the information in **intrusion** detection. ... isolation, user space malicious code **detection**, and policy ...

[Cited by 2](#) - [Related Articles](#) - [Web Search](#)

Google ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [Next](#)

intrusion detection IPC intercept

Search

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

[Ad](#)
[Sc](#)
[Sc](#)

"the" is a very common word and was not included in your search. [\[details\]](#)

Scholar [All articles](#) - [Recent articles](#) Results **1 - 10** of about **1,090** for **database intrusion detection**

All Results

[R Bace](#)
[H Debar](#)
[M Handley](#)
[P Mell](#)
[A Wespi](#)

... of Identifying Vulnerabilities and Patching Software on the Utility of Network **Intrusion Detection** - all 7 versions »

R Lippmann, S Webster, D Stetson - Recent Advances in **Intrusion Detection**: 5th International ..., 2002 - books.google.com

... of the many more machines located **behind a firewall**. ... Signature-based network **intrusion**

detection system will never detect ... in the NIST ICAT meta- **database** [14]. ...

Cited by 43 - [Related Articles](#) - [Web Search](#)

[book] **Intrusion Detection Systems** - all 88 versions »

RG Bace, P Mell - 2001 - motega.com

... Page 3. NIST Special Publication on **Intrusion Detection Systems** Page 3 of 51 ... 35

4.2.1. Location: **Behind** each external **firewall**, in the network DMZ ...

Cited by 175 - [Related Articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#)

... data into a multi-dimensional **database** for network **intrusion detection** and vulnerability assessment - all 3 versions »

R Gleichauf, S Shanklin... - US Patent 6,282,546, 2001 - Google Patents

... with AutoHack-Auditing Security **Behind the Firewall** ... ACM Transactions on **Database Systems**, Mar. ... Short Presentation entitled "**Intrusion Detection** for network ...

Cited by 13 - [Related Articles](#) - [Web Search](#)

Computer network **intrusion detection**, assessment and prevention based on security dependency ... - all 6 versions »

SS Yau, X Zhang - Proc IEEE Comput Soc Int Comput Software Appl Conf, 1999 - doi.ieeecs.org

... 4) Prevention of further **intrusion** The RCs ... security policy, Alice's accounts on **database**

and machine ... have presented an approach to **detection**, assessment, and ...

Cited by 11 - [Related Articles](#) - [Web Search](#)

The use of Honeynets to detect exploited systems across large enterprise networks - all 18 versions »

J Levine, R LaBella, H Owen, D Contis, B Culver - Information Assurance Workshop, 2003. IEEE Systems, Man and ..., 2003 - ieeexplore.ieee.org

... is the use of an **Intrusion Detection System** (IDS ... These signatures normally reside in a **database** associated with ... A Honeynet is a network, placed **behind** a reverse ...

Cited by 54 - [Related Articles](#) - [Web Search](#)

Aggregation and Correlation of **Intrusion-Detection Alerts** - all 12 versions »

H Debar, A Wespi, PT R&D - Recent Advances in **Intrusion Detection**: 4th International ..., 2001 - books.google.com

... new probes or improving the technology **behind** existing ones ... and the alert is stored in a **database**. ... Aggregation and Correlation of **Intrusion-Detection Alerts** 99 ...

Cited by 250 - [Related Articles](#) - [Web Search](#)

[book](#) **Intrusion Detection** with Snort: Advanced Ids Techniques Using Snort, Apache, MySQL, PHP, and Acid - all 3 versions »

RU Rehman - 2003 - books.google.com

... have multiple Snort sensors **behind** every router ... web server on this centralized **database**

server as ... Chapter 1 • Introduction to **Intrusion Detection** and Snort ...

[Cited by 27](#) - [Related Articles](#) - [Web Search](#) - [Library Search](#)

[Scalable, graph-based network vulnerability analysis](#) - all 7 versions »

P Ammann, D Wijesekera, S Kaushik - Proceedings of the 9th ACM conference on Computer and ..., 2002 - portal.acm.org

... 1 and 2). There is an intrusion **detection** system that ... the IDS, but rlogin sessions between hosts **behind the firewall** ... data h : **database** is running on host h ...

[Cited by 115](#) - [Related Articles](#) - [Web Search](#)

[Environmental Key Generation Towards Clueless Agents](#) - all 12 versions »

J Riordan, B Schneier - Mobile Agents and Security, 1998 - Springer

... if the owner of the **database** is watching ... names from hosts inside a domain **behind a firewall** ... dates by backward-time constructs, **intrusion detection** systems which ...

[Cited by 124](#) - [Related Articles](#) - [Web Search](#)

[DARPA Information Assurance Program dynamic defense](#)

[experimentsummary](#) - all 5 versions »

DL Kewley, JF Bouchard, BBN Technol, VA Arlington - Systems, Man and Cybernetics, Part A, IEEE Transactions on, 2001 - ieeexplore.ieee.org

... box hosting the Oracle **database**) was determined ... and, therefore, was not detected **behind the firewall** ... were detected by multiple **intrusion detection** devices, and ...

[Cited by 16](#) - [Related Articles](#) - [Web Search](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google



[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#) | [C](#)

Welcome United States Patent and Trademark Office

[AbstractPlus](#)


[View TOC](#)

[BROWSE](#)

[SEARCH](#)

[IEEE XPLORE GUIDE](#)

Access this document

 Full Text: [PDF](#) (832 KB)

Download this citation

Choose [Citation](#)

Download [ASCII Text](#)

[Download](#)

[» Learn More](#)

[Rights and Permissions](#)

[» Learn More](#)

The use of Honeynets to detect exploited systems across enterprise networks

[Levine, J.](#) [LaBella, R.](#) [Owen, H.](#) [Contis, D.](#) [Culver, B.](#)
Sch. of Electr. & Comput. Eng., Georgia Inst. of Technol., Atlanta, GA, USA;

This paper appears in: [Information Assurance Workshop, 2003. IEEE Systems, Man, and Cybernetics](#)

Publication Date: 18-20 June 2003

On page(s): 92- 99

ISSN:

ISBN: 0-7803-7808-3

INSPEC Accession Number: 7839544

Digital Object Identifier: 10.1109/SMCSIA.2003.1232406

Posted online: 2003-09-23 16:42:44.0

Abstract

Computer networks connected to the Internet continue to be compromised and exploited spite of the fact that many networks run some type of security mechanism at their connec Large enterprise networks, such as the network for a major university, are very inviting ta are looking to exploit networks. Large enterprise networks may consist of many machine: operating systems. These networks normally have enormous storage capabilities and hig bandwidth connections to the Internet. Due to the requirements for academic freedom, sy are restricted in what requirements they can place on users on these networks. The high these networks make it very difficult to identify malicious traffic within the enterprise netw a Honeynet can be used to assist the system administrator in identifying malicious traffic network. By its very nature, a Honeynet has no production value and should not be gene traffic. Thus, any traffic to or from the Honeynet is suspicious in nature. Traffic from the e machine on the Honeynet may indicate a compromised enterprise system.

Index Terms

Inspec

Controlled Indexing

[Internet](#) [authorisation](#) [bandwidth allocation](#) [business communication](#) [comput](#)
[message authentication](#) [network operating systems](#) [system monitoring](#) [telecc](#)
[security](#) [telecommunication traffic](#)

Non-controlled Indexing

[Honeynets](#) [Honeypots](#) [Internet](#) [bandwidth requirement](#) [computer crime](#) [cor](#)
[network](#) [exploited system detection](#) [hacking](#) [intrusion detection](#) [large enterp](#)
[malicious traffic identification](#)

Author Keywords

Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEEExplore.



Login:
 Register

[Home](#) [Browse](#) [Search](#) [My Settings](#) [Alerts](#) [Help](#)

Quick Search Title, abstract, keywords

Author

[search tips](#)

Journal/book title

Volume

Issue

Page

Information Security Technical Report

Volume 3, Issue 4, 1998, Pages 32-42

Font Size:

Abstract

PDF (1422 K)

doi:10.1016/S1363-4127(98)80036-8

Cite or Link Using DOI

Copyright © 1998 Published by Elsevier Science Ltd.

E-mail Article

Export Citation

Cited By

Add to my Quick Links

Save as Citation Alert

Add to

Citation Feed

Request Permission

Feature article

Network-versus host-based intrusion detection

Filip Schepers

Internet Security System (ISS), USA

Available online 12 February 1999.

Related Articles in ScienceDirect

- * Report highlights
Information Security Technical Report
- * Footprinting for intrusion detection and threat assessm...
Information Security Technical Report
- * Introduction
Information Security Technical Report

[View More Related Articles](#)

Information Security Technical Report

Volume 3, Issue 4, 1998, Pages 32-42

[Home](#) [Browse](#) [Search](#) [My Settings](#) [Alerts](#) [Help](#)



[About ScienceDirect](#) | [Contact Us](#) | [Terms & Conditions](#) | [Privacy Policy](#)

Copyright © 2008 Elsevier B.V. All rights reserved. ScienceDirect® is a registered trademark of Elsevier B.V.